Dr. sc. Zdravko Bazdan
E-mail: lujo.bazdan@du.htnet.hr

POSLOVNO-OBAVJEŠTAJNE SLUŽBE, INDUSTRIJSKA I GOSPODARSKA ŠPIJUNAŽA U MEĐUNARODNOJ EKONOMIJI

UDK / UDC: 355.40:339.9
JEL klasifikacija / JEL classification: F50, F53, D83
Pregledni rad / Review
Primljeno / Received: 6. travnja 2016. / April 6, 2016
Prihvaćeno za tisak / Accepted for publishing: 12. listopada 2016. / October 12, 2016

Sažetak

U ovome se radu elaboriraju tri fenomena današnjice a to su poslovno-obavještajne službe, industrijska i gospodarska špijunaža. U uvodnom dijelu objašnjavaju se suvremeni međunarodni odnosi i navode se neka od glavnih tijela OUN-a koja imaju zadatak - uz poštovanje ljudskih prava - stvoriti uvjete za globalni gospodarski rast i društveni razvoj. U drugom dijelu, Subjekti poslovno-obavještajne službe, industrijske i gospodarske špijunaže definiraju se pojmovi uz napomenu da se posebno naznačava razlika između industrijske i gospodarske špijunaže. U trećem dijelu, Metode poslovno-obavještajne službe, industrijske i gospodarske špijunaže, iznose se klasične i suvremene metode kojima se koristi u istraživanju svakoga od spoemnutih fenomena. Zapravo, odnos prema izvorima informacija određuje je li u pitanju legalan ili ilegalan postupak. Zanimljivo je da se nakon disolucije SSSR-a sve razvijene države intenzivno koriste svojim obavještajnim službama kako bi špijunirale konkurente svojih kompanija što su penetrirale u njihove zemlje. Jer, prikupljene informacije im stavljaju na raspolaganje. U Zaključku se rezimira tema, svodeći je na zadaće koje bi u naznačenom kontekstu trebala imati naša politička elita.

Ključne riječi**: CIA, KGB, seks i „medena klopka“, ekonomika, politika, ljudska prava.

1. UVOD

Od 193 zemlje članice OUN-a, prema kriteriju DBP-a, u 2014. gospodarski najmoćnijih deset država bile su: SAD, NR Kina, Japan, Njemačka, Velika Britanija, Francuska, Brazil, Italija, Indija i Ruska Federacija. Njemačka je dugo bila najveća izvoznica na svijetu. U 2014. prema izvoznom kriteriju, prvi deset država bile su: NR Kina, SAD, Njemačka, Japan, Južna Koreja, Francuska, Nizozemska, Hong Kong, Ruska Federacija i Velika Britanija. Važno je znati da je kineski iznadprosječni gospodarski rast bio razlogom povećanju BDP-a, pa je ovaj novi gospodarski kolos u drugom kvartalu 2010. potisnuo Japan na treće mjesto. Tako je NR Kina postala druga navjeća ekonomija na svijetu i našla se odmah iza SAD-a. Ali, ako bi ona nastavila takvim tempom, eksperti predviđaju da bi mogla biti prva ekonomija svijeta za sljedećih trideset godina.[1] Glavne odlike suvremenog razdoblja međunarodne ekonomije su: globalizacija, informatička revolucija i gospodarske integracije. Globalizaciji daju glavni ton transnacionalne korporacije i sedamnaest specijaliziranih agencija OUN-a osnovanih da bi se poboljšalo stanje u nerazvijenim zemljama i razvila međunarodna suradnja temeljena na razmjeni robe i usluga. Sve je to usmjereno na povećanje gospodarskog rasta i društvenog razvoja, uz napomenu da je poštovanje ljudskih prava - neovisno o: rasi, boji kože, spolu, jeziku, vjeri, političkom ili drugom uvjerenju, nacionalnome ili socijalnom podrijetlu - glavni lajtmotiv OUN-a. U tom nizu ističe se Svjetska trgovinska organizacija (WTO) s ukupno 162 države članice, što čini više od 95 posto svjetske trgovine. Dakako, nezaobilazne su i: Međunarodna organizacija rada (ILO), Međunarodni monetarni fond (IMF), Skupina Svjetske banke (WBG) s pet afilijacija, Organizacija UN za prosvjetu, znanost i kulturu (UNESCO), Organizacija za prehranu i poljoprivredu (FAO), ali i Svjetska organizacija za intelektualno vlasništvo (WIPO). Skupa s ostalim specijaliziranim organizacijama i glavnim tijelom OUN-a za područje gospodarskoga i društvenog razvoja, tj. Gospodarskim i socijalnim vijećem (ECOSOC). Uz pomoć svih tih instituacija vodi se politika tzv. odgovorne globalizacije. Naravno da je ta njihova neoliberalistička politika osmišljena i da je vode najrazvijenije, tzv. prve zemlje Skupine Svjetske banke; a službeno su to: SAD, Japan, Njemačka, Francuska i Velika Britanija. Kralježnicom međunarodne ekonomije nazivaju se 34 države članice Organizacije za gospodarsku suradnju i razvoj (OECD).

Sve ovo što je naznačeno odnosi se na ono vidljivo na površini. No, ono što se ne vidi i nije na površini jest žestoki obavještajni rat najrazvijenijih među sobom. To je rat za poslovne informacije[2] i pri tome identična ideološka i politička stajalištima ništa ne znače. Ovaj rat, ponekad na granici političkog incidenta i zategnutih diplomatskih odnosa, posebno se vodi između SAD-a, Japana, NR Kine, Francuske, Velike Britanije, Njemačke i Ruske Federacije. Neke od tih

[1] Falletti, S. 2010. Comment la Chine s'est imposée au monde en 30 ans. *Le figaro*. 17 août. 22.

[2] Prvu poduku o toj temi dao je argentinski profesor međunarodne ekonomije Raúl Prebisch (prvi direktor UNCTAD-a) na predavanjima koja smo slušali u Centru za gospodarski i društveni razvoj zemalja Trećega svijeta (CEESTEM) u Ciudad de México u proljeće 1982.

zemalja češće su u ofenzivi, a neke, poput Njemačke, češće u defenzivi. Ali, jedno je sigurno: najveća su meta SAD, gdje sve gospodarski najmoćnije države svijeta imaju svoje špijune[3] koji za potrebe tih zemalja, ali i njihovih poslovnih subjekata, žele doći do strogo povjerljivih podataka. No, ni SAD ne ostaje dužan U tom smislu ima na raspolaganju najmoćniji obavještajni i kontraobavještajni aparat na svijetu. S druge strane, Japan je s vremenom izgradio sofisticiranu obavještajnu infrastrukturu i u zemlji i u inozemstvu, posebno u SAD-u. NR Kina, koje su se preci u povijesti prvi sustavno koristili obavještajnom službom, ima najbrojniju obavještajnu mrežu na svijetu. Procjenjuje se da su se infiltrirali u sve države visoke tehnologije, posebice u SAD, te da je i to jedan od razloga visoke stope gospodarskog rasta NR Kine.[4] Francuska još od Luja XIV. koristi se mehanizmom obavještajne službe i danas je lider i uzor za *gospodarsku diplomaciju* – u kojoj obavještajna zajednica jedne zemlje ima krucijalnu ulogu. Velika Britanija, skupa sa SAD-om i s još tri razvijene države, Australijom, Kanadom i Novim Zelandom, raspolaže najmoćnijim globalnim špijunskim sustavom na svijetu; one ne ostaju dužne nikomu, a najmanje Francuzima, s kojima tradicionalno zbog toga imaju problema. Njemačka se do sada pokazala suzdržanom u besprizornom i zabranjenom postupku dolaženja do poslovnih informacija i svojim protuobavještajnim sustavom spriječava upade drugih zemalja i njihovih poslovno-obavještajnih službi (*Business Intelligence*) u sustave svojih kompanija.

Doduše, uvijek postoji iznimka koja potvrđuje pravilo. Riječ je o primjeru *Jose Ignazio Lopez v. General Motors*, kad je 1993. J. I. Lopez – kao direktor nabavnog odjela General Motorsa – prebjegao zrakoplovom što ga je unajmio Volkswagen A. G. iz Detroita u Wolfsburg. Tom je prilikom ponio sa sobom dragocjenu tehničku dokumentaciju – što je bio eklatantan primjer industrijske špijunaže. Konačno, u tom je krugu i Ruska Federacija; ona u toj sferi izuzetno agresivno nastupa prema SAD-u, ali i drugim zemljama s visokom tehnologijom. No, Ruska Federacija zbog svojega prethodno već zaustavljenoga tehnološkog razvoja, barem zasad nije od većeg interesa za druge. S druge strane, tradicionalno jaka i iznimno obučena protuobavještajna služba, izgrađena još za vrijeme SSSR-a, evidentan je čimbenik odvraćanja. U posebnu skupinu agresivnih ubrajaju se DNR Koreja, tj. Sjeverna Koreja, i tzv. Islamska Država Iraka i Sirije (ISIS); jedni i drugi svim sredstvima koja im stoje na raspolaganju žele doći do političkih, vojnih i poslovnih podataka. Sjeverna Koreja to radi kako bi napakostila „bastionu imperijalizma“ ubrzanim razvojem svojih vojnih kapaciteta, baziranih na nuklearnom oružju i interkontinentalnim raketama. ISIS to radi prvenstveno kako bi vojno napao SAD u njegovim državnim granicama, ali i na svim točkama u svijetu na kojima se nalaze američki vojnici i civili, te američke instalacije. No, na meti su i njihovi saveznici: Velika Britanija, Francuska, Belgija. Najvažnije informacije do kojih žele doći odnose se na sve vrste sofisticiranih oružja, posebno nuklearnoga i kemijskog, koja bi im omogućila

[3] Unutar obavještajnih zajednica nazivaju se „agentima“ ili „obavještajcima“. A oni koji ne rade za novac, već zbog ideala, nazivaju se „izvidnicima“.

[4] Storelli, C. 2015. US Econonomy at Bay. *International Herald Triubine.* December 21. 3. Paris.

sabotaže i kaos. A vrijeme totalne informatizacije Zapada ISIS-u ide u prilog. I ne samo njima, već i svima onima koji – posebno preko interneta – pokušavaju doći do podataka o onome što ih iz inferiornog može dovesti u potencijalno superioran položaj.

Svima su njima na raspolaganju etični, legalni i legitimni tzv. *otvoreni izvori*. Nadalje, tu su oni neetični, a legalni izvori, tzv. *poluotvoreni izvori*. I na kraju, oni koji žele riskirati kazneni progon, uključujući i višegodišnje kazne zatvora, imaju dostupnima i tzv. *zatvorene izvore*. Ali, organizirano i skriveno od javnosti, u tajnosti njih čeka stotine tisuća, milijuni stručnjaka, znanstvenika, operativaca, doušnika, „krtica", „spavača", kako bi ih onemogućili u nakani. No, u isto vrijeme, jednako tako organizirani i skriveni od javnosti, spremaju za napad u podjednakom broju i jednake stručnosti – oni koji nastoje doći do tajnih informacija. A neki od njih upravo su sada u akciji. Ta interakcija, ti permanentni napadi i obrane sektora istraživanja i razvoja (R & D) javnih i privatnih poslovnih subjekata u najrazvijenijim zemljama - četvrta je dimenzija suvremene međunarodne ekonomije. Riječ je o obavještajnoj i protuobavještajnoj revoluciji, koju vode tzv. prednji odredi i na jednoj i drugoj strani. Važno je naglasiti da je ta revolucija, kao uostalom i sve industrijske revolucije, u prvi plan izbacila neke zemlje, ali i kompanije koje su osnovane poslije svojih najizravnijih konkurenata na svjetskom tržištu, a danas su lideri u svojoj grani. Zašto? Zato što su potukli svoje konkurente i zbog toga što su njihove države i njihovi menadžmenti shvatili navrijeme da bez gospodarske obavještajne službe te gospodarske i industrijske špijunaže ne mogu ostati na vrhu u međunarodnoj ekonomiji. A zemlje poput naše? I one moraju potaknuti ustroj centara za gospodarsku obavještajnu službu u njihovim glavnim poslovnim subjektima i osnovati takve centre u nekima od svojih ministarstava, posebno vanjskih poslova i gospodarstva. Uostalom, u novije doba sve više vrijedi staro pravilo: „Dobra obrana je dobar napad."

2. SUBJEKTI POSLOVNO-OBAVJEŠTAJNE SLUŽBE, INDUSTRIJSKA I GOSPODARSKA ŠPIJUNAŽA

(1) Poslovno-obavještajna služba ima funkciju radara – kako je to običavao reći profesor Stevan Dedijer, jedan od osnivača poslovno-obavještajne službe u svjetskim razmjerima. On je još 1972. počeo zastupati tezu da u vojnu i političku dimenziju obavještajne službe treba uključiti i ekonomski aspekt. Tvrdio je da bez snažne ekonomske baze niti jedna država – pa ni SAD - nema kapacitet optimalnoga vojnoga i političkoga obavještajnog djelovanja. Izuzeće su, dakako, diktature. Tvrdio je da će gospodarska špijunaža biti velika tema 21. stoljeća i da će napredovati samo one države kojima elite to navrijeme shvate.5 Odavno je jasno kako se s pomoću nje dolazi do informacija o intelektualnom vlasništvu konkurenta, dakle o njegovim: autorskim pravima, patentima, industrijskom

[5] Razgovor s profesorom S. Dedijerom u Dubrovniku 1. 4. 1997. U svijetu je nazvan: «osnivačem gospodarsko-obavještajne službe». Organizirani su simpoziji i objavljene knjige u inozemstvu profesoru S. Dedijeru u počast 1983., 1987. i 1992.

dizajnu i poslovnim tajnama, postupcima, tehnologiji i inovacijama. Informacije se prikupljaju iz javnih, tzv. legalnih izvora. A kada ih dijelimo prema izvorima, razlikujemo primarne i sekundarne informacije. Primarni izvori informacija odnose se na sve one čelne ljude koji rukovode određenim poslovnim subjektom čije je poslovanje meta analize. Njihovi nastupi, govori i intervjui posebno se analiziraju. Dakako, zanimljivi su i svi oni koji su na nižim razinama rukovođenja, pa i njihovi nastupi, intervjui i govori podliježu analizi. U skupinu primarnih izvora informacija ubrajaju se i javno dostupna analitička izvješća, ona s redovitih, ali posebno s izvanrednih skupština dioničara.

Sekundarni izvori informacija su: internet, *on line* i digitalne baze podataka, monografije, članci u novinama i magazinima, TV i radijske emisije i sl. Do informacija ovoga tipa može se doći i prateći sajmove, burze (turističke i sl.) i stručne skupove na kojima nastupaju predstavnici određenoga gospodarskog subjekta koji je predmet pozornosti i analize obavještajne službe. Smatra se da legalni izvori čine oko 90 posto traženih informacija. Dakle, da se tolik postotak podataka može naći na takav način.

Nakon klasifikacije informacija, prelazi se na njihovu obradu, gdje se eliminiraju nevažne. Poslije toga slijedi najteža faza a to je analiza informacija i oblikovanje finalnog proizvoda, koji se stavlja na raspolaganje zaduženima za proces donošenja odluka (*Decission Making Process*).

(2) Industrijskom špijunažom (*Industrial Espionage*) dolazi se do informacija koristeći se nelegalnim i neetičnim postupcima. Njome se štede milijarde dolara koje bi inače bilo potrebno uložiti u vlastito istraživanje i razvoj, što je neizvjesno i dugoročno. Inače, špijunaža *per se* može se promatrati s dva aspekta. Prvi je politički, a drugi pravni. U prvome radi se o postupku prikupljanja podataka koje netko skriva. U drugome špijunaža se definira kao postupak što je u nacionalnoj legislativi označen - kažnjivim djelom špijunaže.

Špijunažom se koristi kao sredstvom kako bi se ilegalno „napali" zatvoreni izvori na koje se odnosi dva do tri posto traženih informacija. Dakle, riječ je o kažnjivom djelu špijunaže – konspirativno se služeći ljudima. To je veoma riskantan biznis jer ako se na djelu uhvate krivci za industrijsku špijunažu i ako im se u pravomoćnome sudskom postupku dokaže krivnja, završavaju na višegodišnjim zatvorskim kaznama. Zakonom o gospodarskoj špijunaži SAD-a[6] iz 1996., koji su pripremili senatori Herb Kohl i Arlen Specter, posebno je definiran institut *poslovne tajne*. A paragraf koji se odnosi na to glasi: „Poslovna tajna je svaki oblik i svaka vrsta financijskih, poslovnih, znanstvenih, tehničkih, gospodarskih ili tehnoloških informacija, uključujući obrasce, planove, procedure, programe, ili kodove, vidljive ili nevidljive, bez obzira kako su spremljeni, organizirani ili sačuvani, elektronički, grafički, na fotografijama ili napisani – ako je: (1) vlasnik poduzeo odgovarajuće mjere za očuvanje njihove tajnosti i (2) ako informacije predstavljaju neovisnu ekonomsku vrijednost, aktualnu ili potencijalnu, odnosno ako nisu opće poznate i nisu bile prisutne u javnosti na bilo

[6] Economic Espionage Act (1996), 18 U. S. C., paragraphs: 1831-1839. , Washington, 3.

koji način.“[7] Zakonom određene su i nelegalne i neetične obavještajne aktivnosti:

- nelegalni upadi u tuđe informatičke mreže,
- prisluškivanje telefonskih razgovora,
- lažno predstavljanje ili prikrivanje poradi dolaženja u posjed tajnih informacija,
- nuđenje mita, kompenzacija ili protežiranje neke kompanije u zamjenu za tajne informacije.

Mora se naglasiti da je ovaj zakon donesen prvenstveno zbog stranih vlada pa je špijunažu ovoga tipa podigao na razinu *državnoga kaznenog djela*. Zbog toga osoba koja prikuplja tajne gospodarske informacije u javnim i privatnim gospodarskim kapacitetima u SAD-u u korist inozemne vlade, može se kazniti „novčanom kaznom do deset milijuna dolara ili zatvorskom kaznom do 15 godina“. A kad je u pitanju industrijska špijunaža, kazna iznosi „pet milijuna dolara i/ili zatvorsku kaznu od deset godina“. Prvi koji je 2001. osuđen u SAD-u na temelju ovoga zakona zbog industrijske špijunaže, bio je kineski inženjer Pen Yen Yang.

A što se tiče naše zemlje, materija o ovoj temi nalazi se u članku 262. Kaznenog zakona Republike Hrvatske: „Odavanje i neovlašteno pribavljanje poslovne tajne“:

„(1) Tko neovlašteno drugome priopći, preda ili na drugi način učini pristupačnim podatke koji su poslovna tajna, kao i tko pribavlja takve podatke s ciljem da ih preda neovlaštenoj osobi, kaznit će se kaznom zatvora do tri godine.

(2) Ako je kaznenim djelom iz stavka 1. ovog članka počinitelj sebi i drugome pribavio znatnu imovinsku korist ili je prouzročio znatnu štetu, kazniti će se kaznom zatvora od šest mjeseci do pet godina.“[8]

(3) Ako su definirani pojmovi „poslovno-obavještajna služba“ i „industrijska špijunaža“, ključno je tko sve i kada nastupa kao subjekt. U tom smislu valja razlikovati makro i mikrorazinu aktivnosti. Makrorazina se odnosi na državu koja prikuplja gospodarske informacije na području druge države, bili pritom razlozi političke, vojne ili gospodarske sigurnosti, ili su motivi obavještajni ili protuobavještajni hoće li se te informacije staviti na raspolaganje državnim ustanovama ili se proslijediti nekome od poslovnih subjekata. Razdjelnica je izvor. Naime, ako se to radi uz pomoć zatvorenih izvora, tada je riječ o gospodarskoj špijunaži (*Economic Espionage*).

Od početka 1990-ih godina u međunarodnim odnosima je na djelu novi trend. Temelji su mu nastali nakon rušenja Berlinskog u studenomu 1989., kada je ujedinjena Njemačka.[9] I posebno nakon listopada 1991. kada je u SSSR-u prvo demontiran moćni Komitet državne sigurnosti, tj. KGB. Potom se 26. prosinca 1991. raspao SSSR pa je globalna obavještajna revolucije krenula nesmiljenom žestinom.

[7] Anderson, P. (2009), *Economic Espionage in The World*, Chicago, 56.
[8] Kazneni zakon Republike Hrvatske stupio je na snagu u svibnju 2015. Izvor: http://www.zakon.hr/z/98/Kazneni-zakon
[9] Instruktivan je tekst: „Kohl je od Gorbačova za 15 milijardi kupio ujedinjenje Njemačke“ (2010.), Jutarnji list, 15. listopada, 12.

Zapad je smatrao kako je s političke scene nestala glavna prijetnja svjetskom miru – „Opaki imperij" (*Evil Empire*), kako je SSSR nazvao Ronald Reagan. Stoga su najrazvijenije države prebacile dio ljudskih i materijalnih potencijala iz sektora političke i vojne špijunaže u gospodarsku špijunažu. Kako bi opravdali taj novi trend, ubrzo nakon toga u SAD-u, teoretičari međunarodnih odnosa forsirali su stav kako u suvremenom procesu globalizacije tržišta više nisu u mogućnosti emitirati informacije koje su krucijalne za investitore i njihova ulaganja u kratkoročno, srednjoročno, a posebno u dugoročno razdoblje.

Jednostavno, u situaciji kada zemlje štite svoj nacionalni prostor svim dopuštenim i nedopuštenim sredstvima pa svoje nedaće žele prebaciti na drugoga (*Spillover Effects*), tržište ne može signalizirati ono što je drukčije od merkantilizma. Zbog toga je Laura D'Andrea, potom pročelnica Nacionalnoga gospodarskog savjeta (NEC) u kabinetu Billa Clintona, još 1990. predložila vladi SAD-a da zamijeni filozofiju trgovinske politike i da od koncepta slobodne trgovine prijeđe na sofisticiranu intervenciju korištenjem instrumenata obavještajnih službi. Istaknula je da SAD mora biti spreman onemogućiti konkurente američkih kompanija kad se one bore na tržištu podmićivanjem (*Bribery Attempts*) i tako iz igre izbacuju američke kompanije.[10] Nije napisala, ali je sigurno mislila prije svega na gospodarsku špijunažu, kao popularno sredstvo u podržavanju američkih kompanija u međunarodnoj ekonomiji. Zapravo, špijunirati konkurente nacionalnih kompanija te finalni obavještajni proizvod dostavljati njihovu menadžmentu – postaje jedna od glavnih zadaća čitave obavještajne zajednice SAD-a, sa šesnaest vladinih agencija, od kojih je najpoznatija CIA. No, s tim su se trendom uskladile i ostale najrazvijenije zemalje. A još je 1981. Pierre Marion, direktor francuske obavještajne službe, tj. Glavne uprave vanjske sigurnosti (*Direction Générale de la Sécurité Extérieure – DGSE*) doviknuo Amerikancima: „Kad dođe do biznisa – počinje rat!" Moto da je špijunaža drugi oblik diplomacije, baš kao što je to i rat – uveo je svijet u novu, sadašnju fazu obavještajne revolucije.[11]

Svaka zemlja s inteligentnom vladom trebala bi razraditi gospodarsku strategiju nacionalne sigurnosti[12] u dva podsustava. Prvi je egzogene, a drugi endogene provenijencije. U pogledu egzogenog podsustava riječ je o *sedam čimbenika* koji se odnose na zemlju penetracije kapitala, što je prikazano na shemi 1. To su: korupcija, inflacija, nezaposlenost, insolventnost i nelikvidnost, bijeg kapitala, nepravedna raspodjela dohotka te bijeda, očaj i ksenofobija. Zapravo, svi su ti čimbenici su gospodarsko-socijalni indikatori stanja u zemlji penetracije. Ako se oni približavaju *pragu tolerancije*, nakon čega može doći do političke nestabilnosti, obveza je nacionalne obavještajne zajednice alarmirati o tome involvirane nacionalne poslovne subjekte koji su uložili kroz *inozemne izravne investicije* (FDI).

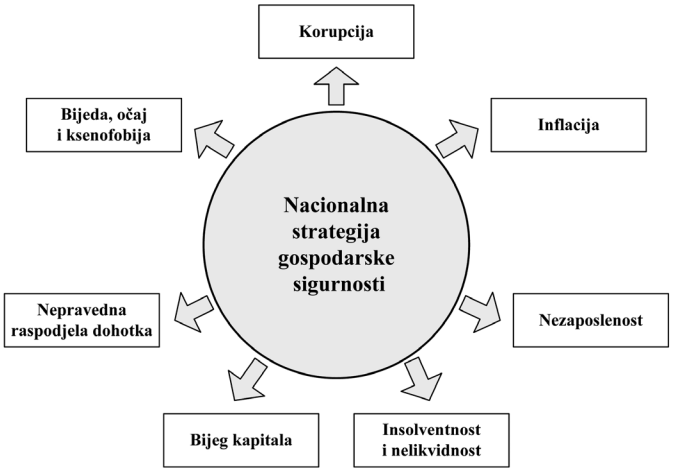
[10] Anderson, Ibid., 59.

[11] Prvu obavještajnu službu na svijetu formirala je 1301. Dubrovačka Republika. Druga je bila ona Venecije, osnovana 1340. Izvor: S. Dedijer, *Ragusa Intelligence and Security 1301.-1806 A Model for the Twenty-First Century?* „International Journal of Intelligence and Counter Intelligence, sv. 15, br. 1, ljeto 2002., 109.

[12] Vlada Republike Hrvatske je na svojoj sjednici od 26. 6. 2003. donijela odluku o pokretanju projekta „Hrvatska u 21. stoljeću". U organizacionoj shemi od 18 ključnih razvojnih područja, izostalo je područje strategije nacionalne gospodarske sigurnosti.

Jer zemlje kojih su poslovni subjekti penetrirali kapitalom i tehnologijom u takva nestabilna područja – nacionalnu gospodarsku sigurnost štite upravo na tim točkama u inozemstvu. Naime, ako dođe do promjene na političkoj sceni u zemlji penetracije - krajnja mjera nove vlasti može biti i višekratna nacionalizacija.[13]

A to je za gospodarske subjekte i njihove vlasnike, od kojih su mali dioničari najbrojniji, katastrofa s nepredvidivim posljedicama. To se upravo proporcionalno odražava i na makroekonomiju zemlje podrijekla izravnih investicija. Doduše, šteta nastaje kada dolazi do poremećaja i kod *inozemnih neizravnih investicija* (FII), tj. kada se masovno i u velikim količinama nezaustavljivo gubi novac na burzama u inozemstvu. I jedno i drugo se, dakako, negativno odražava na zemlju investicija tako što dolazi do opadanja kupovne moći i potražnje za dobrima široke potrošnje i usluga, a nakon toga i do opadanja potražnje za dobrima realne akumulacije. Sve to dovodi do hiperprodukcije, poslije koje nastupa stagnacija, a ako ona potraje - i recesija. A u konačnici vreba - kriza. Doduše, gospodarski poremećaj u jednoj zemlji može nastati i zbog eksternih čimbenika, kada opada potražnja za robama i uslugama širih razmjera. Uz spomenuto, nacionalna obavještajna zajednica ima još i zadaću da stalno prati stanja u zemljama koje su matičnoj državi bitni trgovinski partneri. I ako se ocijeni da dolazi vrijeme gubljena tržišta zbog turbulentnih političkih događaja, budući da se stanje pogoršava korupcijom, inflacijom, nezaposlenošću, insolventnošću i nelikvidnošću, bijegom kapitala, nepravednom raspodjelom dohotka i bijedom, očajem i ksenofobijom – imaju zadaću po svojoj procjeni navrijeme izvijestiti upravu nacionalnih poslovnih subjekata koji posluju u tim zemljama.



Shema 1*. Sedam čimbenika egzogene strategije nacionalne gospodarske sigurnosti zemlje penetracije kapitala

* Dizajn D. Turčinović

[13] Upravo se to dogodilo 1. 5. 2010. u Boliviji Eva Moralesa. Vidi: *Power grab – Another Bolivian nationalization*, (2010), The Economist, May 8th – 14th, 50.

Mikrorazina pritom se odnosi na gospodarske subjekte koji samostalno prikupljaju informacije zbog svojih ofenzivnih i/ili defanzivnih potreba. U tom kontekstu bitno je istaknuti da će oni - ako im nacionalna obavještajna zajednica dostavi svoju procjenu o mogućem gubljenju tržišta zbog političkih promjena u određenoj zemlji – samostalno donijeti odluku. No, uvijek su im na raspolaganju samo dvije solucije. Ipak, važno je naglasiti da svi veliki poslovni subjekti u razvijenim zemljama imaju svoju poslovno-obavještajnu službu, koja prati sve što se događa u najmanje osam područja. Riječ je, zapravo, o čimbenicima ofenzivne strategije inteligentnoga poslovnog subjekta – što je prikazano na shemi 2. To su: konkurenti, inovacije i nove tehnologije, upravljanje ljudskim resursima, istraživanje tržišta, tržište inputa i autputa, burze domaće i inozemne, zakonodavstvo domaće i inozemno[14] te korporativno planiranje ex-ante i ex-post. Nakon te inicijalne faze prikupljanja podataka, oni se, tj. sirove informacije, obrađuju u centru za poslovno-obavještajnu službu. Nakon finalne analize oblikuje se obavještajni proizvod i on se dostavlja menadžmentu. Pri donošenju odluka on ima dva moguća rješenja. Prvo, ostati na tom tržištu i, drugo, dezinvestirati, tj. povući se i penetrirati u treću zemlju.

Shema 2.* Osam čimbenika ofenzivne strategije inteligentnoga poslovnog subjekta

* Dizajn D. Turčinović

I dakle, ako se prikupljaju informacije iz otvorenih izvora, tada se, zapravo, radi o poslovno-obavještajnoj službi supsidijarne jedinice ili o centru poslovno-obavještajne službe lociranom u matičnoj korporaciji. No, ako se podatci prikupljaju iz zatvorenih izvora (kako je već spomenuto), tada se radi o industrijskoj špijunaži. Pritom treba biti fleksibilan, jer ovaj postupak kojim se

[14] Inozemno zakonodavstvo ponekad je također predmetom pozornosti nacionalnih obavještajnih zajednica.

dolazi do tajnih informacija ne odnosi se samo na dva prva sektora gospodarstva, nego i na tercijarni sektor, tj. na bankarsku industriju i osiguranje, pa i na industriju razonode, tj. turizam. Odnosi se, dakako, i na kvartarni sektor, a to su suvremeni transport i suvremene telekomunikacije. Ali, posebno je učinkovit na kvintarnom sektoru, tj. na području istraživanja i razvoja.

Potrebno je naglasiti da je najviše na meti četvrti i peti sektor SAD-a. FBI je još 1992. procijenio da su zbog industrijske špijunaže američke kompanije pretrpjele štetu izgubljenih prihoda u iznosu višemu od 100 milijarda dolara. FBI je 1999. procijenio da je zbog špijunaže Amerika 1997. izgubila oko 300 milijarda dolara vrijedno intelektualno vlasništvo. Najagresivniji industrijski špijuni im dolaze iz: NR Kine, Francuske, Izraela, Japana, Ruske Federacije, Irana i Kube.

Inače, njihova najpoželjnija meta u SAD-u je Silicon Valley, ali i gradovi: Detroit, Dallas, Boston, Washington D. C., Pennsylvania i New Jersey, gdje su proizvođači vrhunske informatičke i komunikacijske tehnologije (ICTs): Cisco Systems, Microsoft, IBM, Hewlett Packard Company, Compuware, Intel, Oracle, Dun & Bradstreet Corporation i sl. Na meti su, dakako, i industrija senzora, aeronautika, naoružanje i energetski materijali. A u tim sektorima zaposleno je više od 40 posto doktora znanosti koji nisu rođeni u SAD-u. I unatoč zaštiti protuobavještajnim mehanizmima, ipak podaci iz SAD-a cure na sve strane i zbog te činjenice; naravno, brojni od stranih zaposlenika postaju industrijski (tehnološki) špijuni, stimulirani prije svega golemim novčanim bonusima. *Vrbuju* se svugdje pa i u trećim zemljama, posebno u njihovim domovinama kada dođu obići roditelje i rodbinu. No, na prvoj crti napada je i Njemačka. Federalni ured za zaštitu ustava (*Bundesamt für Verfassungsschutz – BfV*), glavna njemačka obavještajna agencija, 2009. je procijenio da njihove kompanije zbog industrijske i gospodarske špijunaže godišnje gube 87 milijarda dolara i 30.000 radnih mjesta.[15]

Uz otvorene izvore informacija u tzv. bijelim zonama i zatvorenih izvora u tzv. crnim zonama, postoje i tzv. poluotvoreni izvori informacija u tzv. sivoj zoni.[16] Naime, to je područje gdje se dolazi do informacija na neetičan, ali legalan način. Smatra se da na poluotvorene izvore dolazi sedam do osam posto traženih informacija. No, veoma je tanka crta što razdvaja sivu od crne zone. Do donošenja spomenutog Zakona o gospodarskoj špijunaži, u SAD-u ta je crta bila fleksibilnija i neki postupci prikupljanja podataka su se kvalificirali neetičnima, ali legalnima. Primjer: sovjetski inženjeri su 1974. – u okviru službene kulturno-tehničke suradnje SSSR-a i SAD-a - posjetili Boeing u Seattleu, u saveznoj državi Washingtonu. Cipelama kojima su đonovi bili premazanim posebnim ljepilom donesenim za tu priliku iz SSSR-a i kamufliranim u kutijama kreme za obuću, sovjetski su inženjeri *nehajno* hodali među kompjutoriziranim i robotiziranim strojevima. A zapravo, prikupljali su metalne strugotine specijalnih legura iz kojih su se izrađivali zrakoplovi i svemirske letjelice.

[15] *Behind close doors – A hard struggle to shed some light on a legal grey area*, (2010), The Economist, February 28th – March 6th, 62.
[16] Ibid., 63.

Danas se u svim zemljama takvi postupci smatraju ilegalnima i kažnjavaju se zatvorskim kaznama. A ako su krivci diplomati – osramoćuju se i protjeruju. Godine 1974. završilo je samo diplomatskom protestnom notom koju je State Department uputio Ministarstvu znanosti SSSR-a. I to nakon što su sovjetski inženjeri završili s posjetom SAD-u.

3. METODE POSLOVNO-OBAVJEŠTAJNE SLUŽBE, INDUSTRIJSKE I GOSPODARSKE ŠPIJUNAŽE

3.1. Metode poslovno-obavještajne službe

Metode se baziraju na isprepletenosti empirijskog istraživanja i teorije. Svrha je pronaći ekonomski odnos koji je primaran, prepoznaje trend i utječe na sve ostale relacije. Temelj je prikupiti informacije u postupku „detaljističkog slaganja podataka“ i „stvaranja mozaika“. Pri tome se potrebno služiti metodom za smišljen i standardiziran način obavljanja poslovno-obavještajne djelatnosti, a na raspolaganju su dvije vrste sredstava. Prva su personalna, a druga tehnička sredstva. Personalnima se drže eksperti za pojedina područja, i to za: prikupljanje, provjeravanje i analiziranje te za utvrđivanje vrijednosti i vjerodostojnosti prikupljenih informacija i odvajanja bitnih od nebitnih podataka. Poslovno-obavještajne službe posebice se koriste brojnim tzv. klasičnim metodama, koje se primjenjuju u pojedinim fazama. U prikupljanju informacija to su:

- analiza podataka,
- skladištenje podataka,
- određivanje kvalitete podataka,
- tzv. rudarenje podataka,
- analitičko obrađivanje.

Kako je ovakva aktivnost postala investicijom, a ne troškom jer se uvidjelo da je bez nje nemoguće opstati na svjetskom tržištu, prvi su kadrovi bili umirovljeni obavještajci centralnih obavještajnih službi. Na početku su na najvišoj cijeni bili oni iz: SIS-a, CIA-e i FBI-ja, Mossada, prebjezi iz KGB-a itd. Inače, već dugo je najbolji časopis na svijetu iz ovoga područja onaj Udruženja profesionalaca kompetitivne obavještajne službe (*Society of Competitive Intelligence Professionals - SCIP*) iz Alexandrije, u Virginiji; počeo je 1986. izlaziti u Washingtonu. Prvi im je naslov bio *Competitive Intelligence Review*, a zatim sadašnji *Journal of Competitive Inteligence and Management*. Znači krucijalno štivo za sve one koji se bave poslovno-obavještajnom službom. Spomenuto udruženje se nametnulo i *Etičkim kodeksom za profesionalce konkurentske obavještajne službe,* koji ima sedam točaka. Inzistira se samo na aktivnostima u bijeloj zoni.

Prvo visoko učilište za ove kadrove otvorio je u Parizu 1997. jedan general i dvojica eksperata za ovo područje kao Školu za gospodarsko ratovanje

(*L'Ecole de Guerre Economique*). Obučavaju o „metodama napada i obrane s kojima se suočavaju kompanije u svjetskoj gospodarskoj utakmici". Posebnim se metodama „sirove" informacije podvrgavaju znanstvenoj analizi, kao najtežoj i najdelikatnijoj zadaći svake poslovno-obavještajne službe. Iza toga slijede faze, od kojih je zadnja: uviđanje razvoja budućih događaja. U toj fazi, zapravo znanstvenoj analizi fenomena koji je u fokusu, prognozira se trend kretanja budućih događaja za koje je zainteresiran menadžment. Što se tiče tehničkih sredstava kojima se koristi, to je sofisticirana obavještajna tehnika i suvremena informatička tehnologija.[17]

Prikazat ćemo tri metode kojima se koristi nakon što je formiran obavještajni proizvod. Prvo, riječ je o *analizi scenarija* (*Scenario Analysis*), metodi koja se počela primjenjivati tijekom Drugoga svjetskog rata. Zapravo, osnovna koncepcija povezana je s teorijom ratnih igara (*War Gaming*) i razvila se u vojsci kako bi se predvidjeli budući događaji u vezi s atomskom bombom. U fokusu je analiza vjerojatnog scenarija.[18] Nakon toga, koncepciju je počela primjenjivati uprava američkih transnacionalnih korporacija. Svrha joj je da se procijeni koliko je vjerojatno da će se neželjeni događaj ipak dogoditi. Sredstvo je *ranog upozorenja* (*Early Warning*).

Drugo, riječ je o *Delfi tehnici* (*Delphy Techniques*) . Važno je napomenuti da je u pitanju metoda odlučivanja kojom se u relativno dužem postupku uskladbe stajališta nalazi optimalno rješenje, i to konsenzusom analitičara centra poslovno-obavještajne službe. Naime, rukovoditelj tima koji treba donijeti odluku, finalizira obavještajni proizvod tako da traži od svakog člana pismeni prijedlog rješenja određenoga poslovnog problema. Od sakupljenoga analitičkog materijala pravi se sažetak koji se kopira i prosljeđuje svakom članu tima kako bi svatko sačinio svoj preinačeni prijedlog. Postupak se ponavlja sve dok se postigne konsenzus kojim se želi naći optimalno rješenje. Na taj se način uklanja mogući sukob među analitičarima centra poslovno-obavještajne službe.

Treće se tiče *sustavnog vrednovanja* (*Benchmarking*). U pitanju je metoda kojom se procjenjuje vlastita pozicija na lokalnome, nacionalnome, regionalnome i svjetskom tržištu *vis-à-vis* konkurenciji, posebice u odnosu prema najjačem suparniku. To je, zapravo, postupak određivanja temeljnog standarda proizvoda, ali u usporedbi s najboljim proizvodom konkurenta. Proučava se tako suparnik u nastojanju „da se zaustavi", što je, zapravo, *condicio sine qua non* svakoga poslovnog nadmetanja. Prvi je to korak u poduzimanju akcije. U fazi analize razmatraju se prednosti koje suparnik ima i posebice ljudski resursi i materijalni elementi, rezultati fundamentalnih i aplikacijskih istraživanja što su suparniku omogućili prednost u tržišnoj utakmici.

[17] Mattinet, B., Marti, Y-M. (1995), *L'intelligence Économique – Les yeux et les oreilles de l'enterprise*, Paris, 12.
[18] Donovan, J., W. (1976), *Call for a Central Intelligence Agency*, The Anals of America, sv. 16., 1940-1949, Washington, 393-4.

3.2. Metode industrijske špijunaže

Metodama ove vrste drže se svi oni načini i postupci kojima se koristi subjekt industrijske špijunaže da bi, pod svaku cijenu, došao do željenih podataka. U tom smislu metode se mogu podijeliti na klasične i suvremene. Klasične metodama su postupci povezani s prisluškivanjem i fotografiranjem. Inače, špijuni koji su zaduženi za prisluškivanje, u žargonu CIA-e popularno se nazivaju „muzičarima". Dakle, radi se o:

- prisluškivanju koristeći se „bubama", tj. specijalnim mikrofonima koji nisu veći od zrna graška. Taj sićušni predajnik koji troši dva do tri milivata energije, pri čemu je za emisijski signal dostatan jedan milivat. Sastoji se od tri visokofrekventna i dva nisko-frekventna tonska stupnja. Ima raznih tehničkih varijanata koje uvijek obvezno uključuju minijaturni mikrofon i tonsko pojačalo. Može biti u funkciji oko 100 sati s baterijom od 8,4 volta. Ima osjetljivost na šapat do pet metara, a domet do 500 m. Prijem se može ostvariti i na običnom tranzistoru. Ugrađuje se i u automobil, a priključak upaljača za cigarete može biti izvor napajanja. U ovoj skupini je i:
- mikrofon s pneumatskim pričvršćivačem koji se lijepi na zidove i vrata kako bi se mogli slušati razgovori u susjednoj sobi,
- cjevasti mikrofon koji ulazi u otvor u zidu ili vratima, promjera manjega od milimetra,
- snajper-mikrofonom može se slušati razgovor na udaljenosti i do 500 m. Zapravo, riječ je o relativno malenom uređaju koji se nosi preko ramena, sa slušalicama u ušima i mikrofonom u ljevkastom usmjerivaču koji se drži u ruci i usmjerava na „ciljanu osobu".[19] Također, riječ je o:
- nalivperu, a zapravo ultrakratkom predajniku s ugrađenom antenom dometa od 150 m koji je u funkciji 15 sati, dimenzija 135 x 0,12 mm, težine 25 g s baterijom od 3 x 1,5 volta. Za prijeme se služe i mikrofoni u maslinama zabodenima na *sticku* u koktelima, posebno popularnome kao *Martini dray cocktail*. Ima i mikrofona koji se nalaze u iglama za kravatu. Također, tu je i:
- bešumna minijaturna fotokamera u obliku upaljača za cigarete, veličine 10 cm. U „upaljaču" je špijunska kamera s velikim vidnim poljem i ekspozicijom od pola do tisućitog dijela sekunde; objektiv omogućuje snimanje s udaljenosti od samo 20 cm. Usto ima i:
- tajnoga fotografiranja kamerama što se mogu sakriti čak i ispod košulje, s objektivom postavljenim u iglu kravate,
- tzv. tihe kamere što snima kroz rupicu u zidu ili vratima od samo jednog milimetra,
- tridesetpetmilimetarskih kamera od kojih su najviše na cijeni: Exacta,

[19] Općeprihvaćen termin je i „ciljani objekt". To je objekt prema kojemu je usmjerena obavještajna djelatnost, kao što je npr. sektor istraživanja i razvoja.

Leica, Pentax, Nikon, i Canon. Kositreni Minox prije je za agente bio najpopularniji. Konačno, je tu i:

- „mikrofilmiranje“, pri čemu kamera s malim kasetnim uloškom koja može snimati stranice npr. formata A4 na filmu ne većemu od točke na slovu „i“.

Te su klasične metode i dalje popularne, ali one koje se baziraju na informatičkoj tehnologiji postaju sve važnijima. U tom smislu, industrijska špijunaža posebno se služi tehnikom koja se skupno naziva kompjutorski kriminal (*Computer Crime*) ili kompjutorska špijunaža (*Computer Espionage*). Pripada najsuvremenijim oblicima elektroničke špijunaže. Ti se špijuni koriste kompjutorima koji su prijenos podataka doveli do savršenstva. Poznato je da je kompjutorom sve moguće pa čak i prenijeti velike sume novca s jednoga na drugi račun.[20] Pojavni oblici kompjutorske špijunaže su: otkrivanje poslovne tajne, ilegalni transfer tehnologija, softversko gusarstvo i softverska krađa, tj. *hacking*. A ovo zadnje odnosi se na neovlašteno prodiranje u kompjutorski sustav kako bi se pribavili ekskluzivni dokumenti i podatci. Važno je znati da kompjutor, kad se priključi na internet bez adekvatne zaštite, hakeri mogu „provaliti“ u roku od 40 min. Uz to, kad su u pitanju patološke metode bazirane na informatičkoj tehnologiji, potrebno je spomenuti i metodu ilegalnog transfera tehnologija. Inače, softverska, tj. kompjutorska špijunaža vanjski je uspješna provala u računarske uređaje prisvajanjem intelektualne svojine kopiranjem programa koji imaju svoju licencu, te njihovu predaju konkurenciji ili neovlaštenim osobama. U tim kažnjivim postupcima špijuni prisluškuju, prijemom ili prekidom prijenosa na komunikacijskoj mreži. Procjenjuje se da su 2009. „zločinci širom svijeta načinili ukupne štete od oko 400 milijarda dolara.“[21] No, još jedna krađa postaje sve popularnijom. I pogubnijom za korporacije. To je krađa laptopa (*Laptop Theft*), posebno u zračnim lukama. Naime, prate se „ciljane osobe“ (direktori uprava „ciljanih“ korporacija, direktori sektora za istraživanje i razvoj „ciljnih“ korporacija itd.) i vrebaju njihovi laptopi.

3.3. Metode gospodarske špijunaže

Metode ove treće svi su oni nezakoniti načini i postupci kojima se služe zemlje kako bi došle do željenih podataka. Pri tome zastupljeni su najsuvremeniji postupci i alati. Metode su sofisticirane i alati savršeni. Mogu se podijeliti na klasične i suvremene metode. Prvima se podrazumijevaju oni postupci što se svrstavaju u tzv. tajne operacije (*Covert Operation*) – konspirativnom uporabom ljudi. Ova se metoda prikupljanja tajnih informacija zato i naziva ljudskom obavještajnom službom (*Human Intelligence* – HUMINT). Ti ljudski izvori su: razni profesionalci, informanti, suradnici, tajni agenti, prebjezi, ratni zarobljenici

[20] Kompjutorski je 1997. izvedena prva *velika pljačka banke*. Izveo ju je James McRifkin iz American Software Co. u iznosu od 10,2 milijuna dolara. To „njegova“ banka nije bila primijetila. Upozorio ju je na to FBI. (Izvor: Benett, J. (2013), *Our Fate, Our Ciber Crime*, The New Yorker, October 26, 32.)

[21] Makkoff, J., Barboza, D. (2010), *Researches Spy on Computer Spies, Tracing Dana Theft to China*, The New York Times, April 6, A 1.

i općenito, „špijuni“. Tu su i prikriveni informatori, koji još od *Watergate skandala* iz 1973. nose kodni naziv „duboko grlo“. U ovoj skupini su i specijalisti za „poslove s crnom torbom“, a to su oni što najbolje znaju voditi razgovore u podmićivanju, tj. plaćanju tajnih podataka. U špijunskom žargonu mjesto gdje agent isporučuje mito naziva se „trgovački punkt“. Inače, u žargonu, rezultat špijuniranja je „ulov“ ili „lovina“. Subjekti ove treće skupine su: vrhunski profesionalni obavještajni stručnjaci, agenti, znanstvenici, analitičari, operativci, doušnici i „krtice“. Pritom, ovakva služba ima učilišta za obuka agenata i održavanje veze s agenturom. U pitanju je obrazovanje – među ostalim, i iz područja:

- kriptografije[22], osobnih kontakata, radio-prometa, tehnike ostavljanja poruka na tajnim „javkama“ i tzv. živome tajnom mjestu,
- služenja dezinformacijama i tzv. dvostrukim poigravanjima, uključujući dvostruke agente, dezertere i sl.,
- obučavanja za davanje natrij-pentanola, seruma istine posebno za ispitivanje prebjega,
- uporaba termalnih infracrvena kamera za noćno promatranje i sl.,
- korištenja „gluhim sobama“ za povjerljive poslovne razgovore kao mogućim sredstvom da se onemogućai primjena prislušnih uređaja. One se uglavnom nalaze u sredini objekta. Nemaju prozore kako bi se onemogućilo da se na daljinu (npr. iz susjedne zgrade), preko vibracije prozorskih stakala, prisluškuje razgovor laserskim mikrofonima (*Laser Surveillance System*). [23] Naime, odbijajući se od prozorskog stakla sobe u kojoj se „ciljana osoba“ s jednim ili više sugovornika, laseaski zraka registrira vibracije stakla, a sustav ih prevodi u riječi.

Zapravo, sve ono što se može pročitati u knjigama Iana Fleminga - koji je bio i sam špijun tijekom Drugoga svjetskog rata – događa se i u naše vrijeme. Britanski agent s kodnim imenom „007“ - James Bond, i danas je inspiracija za brojne članove timova koji djeluju kao gospodarski špijuni iza kojih stoji kompletna obavještajna zajednica jedne zemlje. A i o njima je bilo riječi u prvom romanu I. Fleminga iz 1953. pod naslovom *Casino Royal*.

Što se tiče njihova obučavanja, potrebno je istaknuti da se na spomenutim učilištima podučavaju i iz discipline koja nosi naziv – „medene klopke“ (*Honey Trap*), što je drugo ime za „nagovaranje i šaputanje u postelji“. U tom je smislu državna obavještajna služba Njemačke Demokratske Republike - tj. Glavna obavještajna uprava,[24] nekoć nadaleko poznata kao STASI, pod jurisdikcijom Ministarstva državne sigurnosti (*Ministerium für Staatssicherheit - MfS*)[25] - tu metodu dovela do perfekcije. Službu je 1953. utemeljio Markus Wolf – „Misha“, jedan od najtalentiranijih špijuna u hladnom ratu, čelnik državne obavještajne

[22] Vidi zadnji odjeljak glave s naslovom Kriptologija.
[23] O tome više naprijed u okviru mini teme: „suvremeni komunikacijski prijenos“.
[24] U svome sastavu je imala i Znanstveno-tehnološki obavještajni sektor, koji se bavio i gospodarskom špijunažom. STASI je, dakako, imao i protuobavještajnu službu.
[25] Uz ovo ministarstvo postojalo je i Ministarstvo unutarnjih poslova.

službe Njemačke Demokratske Republike. Na njezinu čelu se nalazio 34 godine. Tijekom toga razdoblja obučio je brojne „Romeo"-agente. U svojoj karijeri M. Wolf je infiltrirao u NATO oko 4 000 špijuna. Njegov je agent bio i Günter Guillaume, u Zapadnu Njemačku poslan 1956. Postao je pomoćnik njemačkog kancelara Willyja Brandta, a kada se 1974. to doznalo, W. Brandt je morao dati ostavku. U obavještajnoj akademiji odvajani su najzgodniji i najljepše građeni pitomci. Po posebnom programu, koji je trajao još četiri semestra, morali su ovladati svim finesama u zavođenju. To je pretpostavljalo: poznavanje bontona, usavršavanje socijalnog komuniciranja, učenje o gastronomiji, enologiji, pripravljanju kratkih i dugih koktela, te poznavanje klasične literature i glazbe. No, to i nije bilo najvažnije. Najbitnije je bilo poznavati najširi repertoar seksualnih tehnika koje su se učile i iz *Kåme sŭtra*. A da bi bili u što boljoj fizičkoj kondiciji, svakodnevno su vježbali u teretanama i plivali u bazenima. Tako neodoljivi, na meti su im bile sekretarice, posebno one srednjih godina, zaposlenice u NATO-u koje su dolazile u kontakt s dokumentima s oznakom „*Cosmic"* ili „*Top Secret"*. Na meti su, također, bile tajnice u njemačkim državnim ustanovama i privatnim kompanijama. M. Wolf je znao reći: „Stvar je u tome da su tajnice ministara ili generala uglavnom žene i da kroz njihove ruke prolaze podaci kakvima najčešće ne raspolažu državni tajnici ili članovi vlade. One su bile naši najbolji donosioci državnih tajna."[26]

Dakako, i danas su u uporabi metode „medene klopke". Na meti gospodarske špijunaže su zbog dragocjenih *insajderskih informacija* posebno poslovne tajnice državnih ustanova i korporacija. Ipak, za razliku od *STASI modela*, danas su u ovaj „posao" više uključene žene. Vraćajući se u povijest, naveli bismo glasovitu Matu Hari, nizozemsku plesačicu, kurtizanu i špijunku koja se pročula prije Prvoga svjetskog rata kao plesačica erotskih plesova po prijestolnicama Europe. A kad je počeo Veliki rat, počela je odvlačiti u postelju francuske generale kako bi doznala francuske vojne, političke i gospodarske tajne To ju je koštalo glave pa je 1917. u Parizu strijeljana kao njemačka špijunka. U špijunskom žargonu – žena zavodnica koja treba navesti muškarca u „medenu klopku" naziva se – „Lastavica". A „lastavičje gnijezdo" je, zapravo, stan opremljen kamerama i videoopremom kako bi se žrtva kompromitirala, ucijenila i prisilila na „kooperativnost".[27] Jedan primjer: afera koja je 1963. potresla Veliku Britaniju bila je povezana sa špijunskom aferom u kojoj je krivac bio John Profumo, ministar obrane u konzervativnoj vladi Harolda Macmillana. „Lastavica" je bila Christine Keeler, lijepa ruska špijunka. Kad je afera postala javnom, pala je vlada Harolda Macmillana i došlo je do prijevremenih parlamentarnih izbora. Za poslove špijuniranja koristi se, dakako, i muškarcima homoseksualcima. U istom žargonu, homoseksualac koji namamljuje u homoseksualnu „medenu klopku" radi ucjene, ima kodno ime – „Tihi".

Suvremene metode zahtijevaju najsuvremenije alate. Kad se špijunažom dolazi do tajnih informacija uporabom tehničkih sredstava, radi se o tehničkoj

[26] Obituary*: Markus Wolf*, (2006), The Economist, November 18th - 24th, 86.
[27] U žargonu KGB-a ti prostori su imali kodno ime „Malina".

obavještajnoj službi (*Technical Intelligence* – TECHINT). Te su metode napredovale divovskim koracima, posebno uz pomoć satelita. Dakle, tajne informacije prikupljaju se tehničkim sredstvima u procesu nadzora neprijateljskih sredstva veze. Pa ipak, ljudski su izvori i dalje krucijalni izvor. M. Wolf tvrdi: „Mislim, ipak da rad s ljudskim izvorima – tako dugo dok te službe postoje – nikad neće biti moguće u potpunosti nadomjestiti. Tehničkim sredstvima samo se približno može ustanoviti trenutačno stanje na prostoru što ga se nadzire. Tajni planovi, opcije, i odluke ostaju skriveni i za najrazvijenije satelite.“[28]

A kad je u pitanju tehnička obavještajna služba, nekoliko je njezinih segmenata, od kojih ćemo objasniti tri. [29] To su:

- Obavještajna služba veze (*Signal Intelligence – SIGINT*). Definira se kao ustrojbena jedinica sa zadaćom prikupljanja obavještajnih podataka presretanjem elektroničkih signala koji su rezultat komunikacije među ljudima. U tim okolnostima radi se o komunikacijskoj obavještajnoj službi (*Communications Intelligence – COMINT*).
- Ako je riječ o obavještajnim podatcima sakupljenima presretanjem elektroničkih signala koji nisu izravno korišteni u komunikaciji među ljudima – tada je to elektronička obavještajna služba (*Electronic Intelligence – ELINT*).

No, obavještajna služba veze može biti kombinacija i jedne i druge službe. A kako je riječ o osjetljivim i povjerljivim informacijama koje su obično kriptografirane, tada obavještajna služba veze uključuje dekriptažu. Zbog toga će se zadnji segment ovog poglavlja odnositi na dvije teme. Prva je obavještajna služba veze na primjerima, a druga kriptologija. [30]

(i) Za obavještajnu službu veze važno je naglasiti kako je danas na djelu državna elektronička špijunaža. Imaju je razvijene države, ali i neke koje to nisu. Primjer je Kuba. Naime, u Lurdesu, mjestu nedaleko od Havane, do 1992. bila je smještena najveća sovjetska prislušna i špijunska instalacija izvan granica SSSR-a. Nakon toga, preuzeli su je Kubanci. Izvana, to je poljoprivredna farma u kojoj radi 2 000 tehničara. Instalacije se sastoje od: goleme antene, velikih satelitskih prijamnih terminala u obliku tanjura, mikrovalnih releja sustava goleme brzine i 50 zgrada s opremom koja služi za praćenje, obradu i analizu podataka. Na meti je posebno SAD, koji je samo 90 milja (140 km) udaljen od Kube.

Danas se suvremeni komunikacijski prijenos obavlja u jednomu integriranom sustavu. Karakterizira ga kombinacija žičanoga, tj. kabelskog, i bežičnoga, tj. zračnog ili kozmičkog prijenosa. Dostatno je prisluškivati samo jedan telefonski broj da bi bili prisluškivani i svi ostali koji telefonom komuniciraju s „ciljanom osobom“. Satelitska i mobilna telefonija pruža i te mogućnosti, ali može locirati ta kretanja skupa s naziranom osobom. Nadalje,

[28] Wolf, M. (2004.), *Čovjek bez lica,* Zagreb, 310.
[29] Akronimi ostalih su: GEOINT, FISINT, MASINT i IMINT.
[30] Grč. *krýptō* – skrivam, pokrivam i lat. *lógos* – riječ, govor.

prisluškivani se prisluškuje i kada mu telefon nije uključen. Suvremena tehnika omogućava da se iz službe koja prisluškuje nazove broj mobilnog telefona „ciljane osobe“ te da se, prije nego se pritisne zadnji pozivni broj, ubaci posebna šifra za uključivanje mikrofona mobilnog telefona te osobe. Tako mobilni telefon postaje „buba“ i prenosi sve zvukove u radijusu od 15 m. Ta vrsta prisluškivanja mogla se onemogućiti vađenjem baterije iz mobilnog telefona. Međutim, u Velikoj Britaniji razvijen je tzv. digitalni *System X* koji prati i prisluškuje i isključene mobilne telefone. Mogu se pratiti ujedno i svi razgovori u okruženju „ciljane osobe“. Navedenom se tehnikom prati na stotine milijuna ljudi i mobilnih i satelitskih telefonskih razgovora njihovih korisnika. Uz to, baza podataka digitalnog *Systema X* čuva informacije i do šest mjeseci. Uzgred rečeno, na traženje Ruske Federacije, a potom NR Kine, sustav je prvo bio prodat njihovim tajnim službama.

U upotrebi su još uređaji za prisluškivanje mobilnih telefona CAS – 800. Automatski se uključuju na zadani broj ili zadanu riječ. Mogu i grafički locirati mjesto na kojemu je telefon s kojeg se razgovara. Također, u njemu se nalazi i tzv. *periferna oprema* GCOM – 4510 LSS (naprijed spomenuti *Laser Surveillance System*)[31] koji ispušta laserski zrak dometa 300 do 400 m. Njime se prate razgovori koji vodi „ciljana osoba“.

Dat će se nekoliko primjera *kozmičke špijunaže*.

- ECHELON je najveći globalni multinacionalni špijunski sustav takva kodnog imena. Utemeljen je tajnim ugovorom iz 1948. između SAD-a i Velike Britanije kao UKUSA, kako bi se kontrolirao SSSR. Poslije je dobio i druge zadaće, pa ih ima i danas. Obuhvaća čitavu Zemlju i seže u svemir. Sastoji se od 120 špijunskih satelita i pet prislušnih centara na teritorijima zemalja članica, te od četiri tisuće prijamnih stanica postavljenih na svih sedam kontinenata. Američka Nacionalna agencija za sigurnost (NSA) upravlja ECHELON-om iz Fort Meada u Marylandu.
- „FRENCHELON“ je kolokvijalno ime za francuske kapacitete *Signal intelligencea*. Najveći su poslije ECHELON-a. Ovaj sustav elektroničke špijunaže raspolaže drugom najrasporostranjenijom mrežom izviđačkih baza na svijetu. Najveća se postaja nalazi u francuskom gradu Domme, u blizini Surlata u Périgordu. Imaju i supertajni centar Mutzig, nazivan Centar za elektroničko ratovanje (CGE).
- WATSON[32] SYSTEM američki je moćni suvremeni programski softver. Analitički je sustav za elektroničku špijunažu, dekodiranje i analizu svih vrsta komunikacija digitalne i mobilne telefonije. Početkom listopada 2001. ustupljen je Republici Hrvatskoj radi regionalne kontrole komunikacijskih sustava središnjeg i južnog dijela Europe.

[31] Makedonska vladajuća stranka VMRO-DPMNE je 1998. dobila na dar četiri ovakva uređaja od naše Službe za zaštitu ustavnog poretka (SZUP). SZUP je prethodnica naše današnje središnje Sigurnosno-obavještajne agencije (SOA).

[32] Nazvan je po prezimenu pomoćnika Sherlocka Holmesa.

- GALILEO je satelitski sustav Europske unije i Europske agencije za svemirska istraživanja. Nastao je kao reakcija na spoznaju o ECHELON-u i način je oslobađanja pozicije korisnika američke tehnologije i želje za uspostavom stvarnog suvereniteta nad europskim prostorom. Prva raketa koja je ponijela u svemir prvi satelit sustava GALILEO (GSTB-V1), lansirana je 2004.[33]

I kao što je naznačeno u uvodu, danas svi špijuniraju svakoga. Evo samo četiri primjera:

- I Britanci se žale na Amerikance. Pa iako su 1948. oni skupa osnovali ECHELON, sustavom se u proteklom razdoblju više puta koristilo za špijuniranje i britanskih kompanija. *Independent of Sundy* je u srpnju 1994. izvijestio da je administracija Billa Clintona u razdoblju od siječnja 1993. - kada je stupio na dužnost - do lipnja 1994. prikupila informacije o dodjeli međunarodnih ugovora vrijednih 30 milijarda dolara, te o inozemnim pretendentima na te ugovore koji su se odnosili na poslove iz aeronautike, telekomunikacija i energetike. Te informacije bile su dane američkim kompanijama.
- Boeing 767-300 proizveden je bio za kineskog predsjednika Jiang Zemina i isporučen je 2000. Poslije se otkrilo da su u Boeing Amerikanci ugradili 27 prislušnih uređaja koji emitiraju signale prema satelitima.
- Krajem iste, 2000., zbog mobilne je špijunske afere došlo do poremećaja diplomatskih odnosa između Francuske i Velike Britanije. Naime, MI5 je pokrenula istragu o francuskome gospodarskom špijuniranju najvećih britanskih kompanija. Radilo se o britanskoj kompaniji za mobilnu telefoniju Orange, koju je za 31 milijardu funta iste godine kupio France–Telekom. Zapravo, francuska obavještajna služba, tj. Glavna uprava vanjske sigurnosti, za vrijeme pregovaranja o prodaji kompanije Orange – osigurala je tajne podatke na osnovi kojih je France–Telekom ostvario prednost nad američkim kupcem, pa je tako preuzeo britansku mrežu mobilne telefonije.
- U srpnju 2009. kineske vlasti su u Shanghaiu uhapsile četveročlanu upravu supsidijarne jedinice australijske transnacionalne korporacije Rio Tinto Group, optuživši ih za potkupljivanje i industrijsku špijunažu. Prvooptuženi Australijanac bio je podrijetlom Kinez, a ostali su bili kineski državljani. Optuženi su i za „krađu komercijalnih tajna". Prvooptuženi je u ožujku 2010. osuđen na deset godina zatvora. Zapravo, ovim se primjerom željelo upozoriti na činjenicu kako ni jedna zemlja nije lišena toga da bude metom industrijske i/ili gospodarske špijunaže. Tako ni NR Kina, za koju se procjenjuje da u svijetu ima oko milijun aktivnih špijuna, uključujući i „spavače".[34]

[33] Anderson, P. Ibid., 59.
[34] Russel, T. (2010), *Russia had only hundreds of thousands of agents, compared with China's 1 million*, The Washington Times, February 15, 4.

(ii) Kriptologija je znanstvena disciplina o prikrivanju informacija u porukama. Dijeli se na dva podsustava: kriptografiju i kriptoanalizu. Kriptografija je znanost i vještina u zaštićivanju podataka. Prvo se informacija pretvara u oblik koji je čini neupotrebljivom. To je faza šifriranja ili enkripcije (kriptaže). U ovlasti je obrade *šifranata*. Potom se ponovno vraća u izvornu informaciju, tj. u otvoreni tekst (*Plaintext*). To je faza dešifriranja ili dekripcije (dektiptaže), kada se nastoji „probiti šifra". Proizvod kriptografije je kriptogram. Drugi podsustav je kriptoanaliza. To je znanost kojom se proučavaju metode za otkrivanje izvorne informacije u kriptogramu, a da se ne poznaje *ključ*, tj. *kôd*.

Inače, kriptogram je tajno pismo u kojemu se sustavno razmještaju ili zamjenjuju grafički znakovi kako bi tekst postao nerazumljiv za „neprijatelja". Radi se o zamjeni, tj. šifriranju slova, slogova ili riječi, a ponekad i čitavih rečenica. Zamjena se provodi po nekom pravilu uz pomoć različitih znakova, slova, riječi, izraza i sl. Tekst se može pročitati, tj. može se svesti na izvorni, *otvoreni tekst* samo uz primjenou *kôda*, tj. *ključa* ili *baze šifriranja*. Za šifriranje i dešifriranje služe posebni rječnici, tj. kodeksi. Zbog toga već dugo vojni štabovi, ministarstva vanjskih poslova, ministarstva gospodarstva, diplomatska i druga predstavništva, a već duže i poslovno-obavještajne službe u sastavu svojih stručnih službа – imaju „odsjeke za šifru" i kriptografske stručnjake. Inače, među njima su najbrojniji matematičari, elektroničari i lingvisti. Ti se stručnjaci nazivaju kriptolozima ili šifrerima. Dakle, njihova je zadaća šifrirati i dešifrirati poruke. Inače, digitalni kompjutor za potrebe dešifriranja neprijateljevih poruka izumio je 1944. Howard Aiken, profesor s Harvarda. Nazvao ga je Marc 1.

U ovom području na svijetu je najjača već spomenuta američka Nacionalna agencija za sigurnost, koja ima tri centra: Upravu za istraživanje i razvoj, najvažniju za kriptoanalizu, Upravu za tajnost komunikacija i Upravu za istraživanje, razvoj i usavršavanje sustava za prijenos informacija u komunikacijskim sustavima. Inače, iz matematike i fizike kriptoanaliza uzima teorijske osnove za svoju izgradnju pa se na kompjutorima simulira rad novodizajniranih šifara. One koje zadovoljavaju kriterije zaštite tajnosti, iz istraživačke faze prelaze u razvojno-proizvodnu. Tada se određuju norme za šifriranje i dešifriranje koje se moraju zadovoljiti. Nakon toga se oblikuje proizvod i plasira se na tržište. Koliko u njemu ima „stražnjih vrata" (*Backdoor, Trapdoor*)[35] – ostavlja se korisnicima da ih otklone i nađu ako to mogu. Kako bi se olakšao postupak šifriranja, čitanja i kriptoanalize, na tržištu se danas mogu nabaviti elektronički kriptografski uređaji za šifriranje i dešifriranje. U tom pogledu poznat je sustav Crypto AG Helvetica; njega su preuzeli Siemens i Motorola. Uz ove transnacionalne korporacije takve sustave danas proizvode Transvertex iz Švedske i Nokia iz Finske. Ipak, cijela svjetska industrija naprednih softvera i dogradnja „stražnjim vratima" danas se nalazi pod kontrolom Nacionalne agencije za sigurnost. SAD odbija mogućnost da inozemnim partnerima interneta dopusti prodaju kriptografskih sustava s ključem koji prelazi 56 bita. Tako su svi – posebno Europa – primorani ulagati u

[35] Proizvođač namjerno ugrađuje tajni pristup sustavu zbog mogućnosti upada i potrebe nadzora.

vlastiti razvoj kriptografskih sustava. Kao posljedica toga, Institut za društvena istraživanja i veze (IRCS) u Torinu, koji se bavi internetskim-komunikacijama, razvio je svoj poznati sustav za zaštitu dokumenata ERMES. Inače, smatra se da je industrija kompjutorske zaštite (*cyber-security industry*) jedna od najkonjunkturnijih industrija današnjice. „Bank of America Merrill Lynch (najveća je transnacionalna bankarska korporacija na svijetu – Z. B.) u svojemu nedavnom izvješću procjenjuje da današnje tržište kompjutorske zaštite iznosi godišnje 75 milijarda dolara, a da će iznositi 170 milijarda dolara do 2020.“[36]

4. ZAKLJUČAK

Na kraju Uvoda bilo je naglašeno da je obavještajna revolucija, „kao uostalom i sve industrijske revolucije, u prvi plan izbacila neke zemlje i kompanije koje su na svjetskom tržištu osnovane poslije svojih najizravnijih konkurenata, ali koje su danas lideri u svojoj grani“. Zato se postavlja pitanje zašto je to tako kad oni prvi redovito i imaju prednost. Odgovor glasi: Zato što su njihovi menadžmenti rano shvatili da bez poslovno-obavještajne službe te gospodarske i industrijske špijunaže ne mogu opstati u sukobu sa žestokom konkurencijom na međunarodnoj poslovnoj areni.

U liderskim zemljama, kao što su prije svega: SAD, Japan, Njemačka, Francuska, Velika Britanija, Kanada, Izrael, Nizozemska, Danska, Finska, Norveška i Švedska, dolazi do rapidnih promjena u poslovnoj filozofiji, pa tako i u strukturi proizvodnje. Shvatilo se da više nije dostatno proizvoditi što više i jeftinije jer se time povećavaju troškovi skladištenja. Danas se optimalna strategija bazira na racionalnoj proizvodnji gdje menadžment stalno prosuđuje potrebe tržišta, tragajući za određenom skupinom potrošača (*Niche Marketing*), na čije zahtjeve promptno reagira. U isto vrijeme prate se postupci konkurenata i razvoj njihove proizvodnje, ponude inputa i usluga. Upravljanje kadrovima i znanje postaju najvažnijima. *Jer, danas i najveća kompanija može opstati ako joj se promijeni vlasnička struktura kapitala. No, ukoliko se zaustavi, ili kolabira središnji informatički sustav – atrofira čitava kompanija*. Promjena načela organizacije je dokaz da u tehnološki najrazvijenijim zemljama prelaze *iz klasičnog kapitalizma u ekonomiju znanja*. Osnovni čimbenici ekonomije znanja su povezanost motivacije, ljudske kreativnosti i znanja i, kao rezultat toga, razvoj mrežne industrije (*Network Industries*). Tu je informatička i komunikacijska tehnologija dostupna svima,[37] uz umreženost i povezanost u sustav radi jeftinije i brže razmjene informacija i znanja. Globalno tržište i *outsourcing*, inspirativno poslovno okruženje, laka dostupnost kapitala i mobilnost rada baziranoga na znanju, gdje su troškovi umnožavanja proizvodnje nešto viši od nule, a gdje na usluge, u okviru realne ekonomije, otpada sve veći dio GDP-ja – glavne su odlike te nove potentne ekonomije.

[36] *Cyber-securitu: The cost of immunity* (2016), The Economist, November 7th-13th, 59.

[37] Pretpostavlja se da će ovaj sektor do 2018. stvoriti 6,8 milijuna novih radnih mjesta u svijetu, a u iduće četiri godine da će se registrirati novih 75 000 IT kompanija. Izvor: Lynch, S. (2015).*Turn off – drop out*, New York Post, May 3, 28.

Na kraju ove teme postavlja se ključno teorijsko, ali i praktičnopolitičko pitanje a što je sa zemljama poput naše. Kako se one snalaze i kako da krenu naprijed? Odgovor treba tražiti u činjenici da i one trebaju prilagoditi strategiju razvoja uz pomoć ekonomije znanja. U toj novoj strategiji mjesta mora biti za ustroj centara gospodarsko-obavještajne službe na makro i mikrorazini. Odgovor treba tražiti i u tuđim pozitivnim primjerima, kakvi su japanski,[38] južnokorejski i francuski. U tim je zemljama još prije više desetljeća u poslovnu filozofiju ugrađena maksima prema kojoj ulaganje u poslovno-obavještajnu službu nije trošak – nego investicija. No, zaokružena moderna strategija gospodarskog rasta i društvenog razvoja mora sadržavati još jednu ključnu kariku, a ta karika već je spomenuta *gospodarska diplomacija*. Danas je jasno da nam nema gospodarskog rasta bez gospodarske diplomacije, u kojoj naša obavještajna zajednica mora imati fundamentalnu ulogu. Izvršnu ulogu u tome trebaju imati naši najistaknutiji političari na čelu s Predsjednicom Republike. Oni moraju postati naši glavni poklisari u međunarodnoj ekonomiji – ne oklijevajući da na svjetskom tržištu u svakoj prilici zastupaju interese naših poslovnih subjekata, prethodno brifirani od vodstva naše obavještajne zajednice.[39] Moraju se ugledati u bivšeg predsjednika Francuske Republike Jacquesa Chiraca, koji je 1997. utemeljio matricu ponašanja najviših političkih dužnosnika svake zemlja, kada je izjavio: „Kad putujem u inozemstvo nemam nikakvih predrasuda. Idem prodavati francuske proizvode!“[40] Dakako, prethodno u suglasju s vodstvom francuske obavještajne zajednice.

LITERATURA

Anderson, P. 2009. *Economic Espionage in The Worl.* Chicago.

Behind close doors – A hard struggle to shed some light on a legal grey area. 2010. *The Economist.* February 28th – March 6th.

Benett, J. 2013. Our Fate, Our Ciber Crime. *The New Yorker*. October 26.

Cyber-securitu: The cost of immunity. 2016. *The Economist.* November 7th-13th.

Dedijer, S. 2002. Ragusa Intelligence and Security 1301.-1806 A Model for the Twenty-First Century?. *International Journal of Intelligence and Counter Intelligence*, sv. 15, br. 1, ljeto 2002.

Donovan, J. W. 1976. Call for a Central Intelligence Agency. *The Anals of America*. sv. 16., 1940-1949. Washington.

Economic Espionage Act. 1996. 18 U. S. C., paragraphs: 1831-1839. Washington.

[38] U godini završetka Korejskog rata, tj. 1953., Jugoslaveni su imali veći nacionalni dohodak *per capita* od Japanaca.
[39] Kod nas postoje objektivne zapreke, a to je nastavni kadar. Izvor: B. Javorović, N. Bilandžić, *Poslovne informacije i business intelligence*, Zagreb, 2007., str. 288. Radi se o prvom najboljem djelu na ovu temu. Recenzirali su ga: M. Tuđman i Z. Bazdan.
[40] Sidibé, D. i Saner, R. 2012.The Intersection Between the Roles oft he State and of Multinationals, u: *Business, Society and Politics: Multinationals in Emerging Markets*. Ur. A. Hadjikhani, U. Elg, P. Ghauri, Bingley, 330-1.

Falletti, S. 2010. Comment la Chine s'est imposée au monde en 30 ans. *Le figaro*. 17 aoút.

Kohl je od Gorbačova za 15 milijardi kupio ujedinjenje Njemačke. 2010. *Jutarnji list* 15. listopada.

Lynch, S. 2015. Turn off – drop out. *New York Post*. May 3.

Javorović, B., Bilandžić N. 2007. *Poslovne informacije i business intelligence*. Golden marketing. Zagreb.

Makkoff, J.; Barboza, D. 2010. Researches Spy on Computer Spies, Tracing Dana Theft to China. *The New York Times*, April 6.

Mattinet, B., Marti, Y-M. 1995. *L'intelligence Économique – Les yeux et les oreilles de l'enterprise*. Paris.

Power grab – Another Bolivian nationalization. 2010. *The Economist*. May 8th – 14th.

Obituary*: Markus Wolf*. 2006. *The Economist.* November 18th - 24th.

Sidibé, D.; Saner, R. 2012. The Intersection Between the Roles oft he State and of Multinationals. U: *Business, Society and Politics: Multinationals in Emerging Markets*. Ur. A. Hadjikhani, U. Elg, P. Ghauri. Bingley.

Russel, T. 2010. Russia had only hundreds of thousands of agents, compared with China's 1 million. *The Washington Times*. February 15.

Storelli, C. 2015. US Econonomy at Bay. *International Herald Tribune*. December 21. Paris.

Wolf, M. 2004. *Čovjek bez lica.* Zagreb.

http://www.zakon.hr/z/98/Kazneni-zakon (preuzeto 7. 3. 2016.)

Zdravko Bazdan, PhD
E-mail: lujo.bazdan@du.htnet.hr

BUSINESS INTELLIGENCE, INDUSTRIAL AND ECONOMIC ESPIONAGE IN INTERNATIONAL ECONOMY

Abstract

This work elaborates three phenomena: business intelligence, industrial and economic espionage. The introduction begins with an elaboration of the contemporary international relations. Some of the most important elements of the UN which have the task of creating conditions for global economic growth and social development with human rights approach are also addressed. In the second part, under the title Subjects of business intelligence, industrial and economic espionage, terms are defined. The difference between industrial and economic espionage is evaluated. In the third part, under the title Methods of business intelligence, industrial and economic espionage, classical and contemporary methods used in investigation of the mentioned phenomena are elaborated. It is important to note that after the USSR dissolution, all developed countries used their secret intelligences to spy on competitors. Gathered information was of great benefit to them. In conclusion, the topic of secret intelligence is summarized, leading to the tasks which our political elites would need to attain in the mentioned context.

Key words: CIA, KGB, sex and „honey trap", economics, politics, human rights

JEL classification: F50, F53, D83